IN THE UNITED STASTES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA, *Plaintiff*, v. MICHAEL GOLIGHTLEY, *Defendant.*	)	Case No.: 18-10097-JWB

MEMORANDUM AND ORDER

This matter came before the court on March 21, 2019, for an evidentiary hearing on Defendant's motion to suppress (Doc. 25.)[1] The motion has been fully briefed and the court is prepared to rule. (Docs. 30, 32.) For the reasons stated herein, Defendant's motion is DENIED.

I. Facts

Defendant is charged with seven counts of intentional damage to a protected computer, 18 U.S.C. § 1030(a)(5)(A) and one count of threat to damage a protected computer, 18 U.S.C. § 1030(a)(7). On May 23, 2017, Jeffrey Ridgway, an investigator with the Hays Police Department, presented an application for a search warrant to Ellis County District Judge Glenn Braun. Ridgway sought a warrant for 714 1/2 Topeka Street, Larned, Kansas, to search for items that were evidence of a violation of K.S.A. 21-5839, specifically computers, laptops, cellular phones, tablets, or other mobile devices capable of being used to access the internet based Nex-Tech Classified system. Officers executed the search warrant for 714 1/2 Topeka Street on May 24. 714 Topeka Street is

[1] At the hearing, Defendant requested that the court delay ruling on this motion and allow him through Friday, March 29, 2019, to file a supplemental brief raising new issues that may have arisen at the hearing. The court granted the request, but Defendant elected not to file a supplemental brief.

a residence that is modified into three apartments. (Doc. 25 at 1.) 714 1/2 Topeka is one of the three apartments at the residence. (*Id.*) Immediately after searching 714 1/2 Topeka Street, on May 24, 2017, Ridgway, presented a second application for a search warrant to Judge Braun. This warrant was to search the shed behind 714 Topeka Street. The second affidavit is nearly identical to the first affidavit. Therefore, the court will generally refer to both affidavits as "affidavit" throughout this order. Ridgway's affidavit included extensive statements regarding the investigation. Instead of quoting the relevant portions, the court will summarize the affidavit.

Nex-Tech provides internet services and runs a classified advertisement service that is known as Nex-Tech Classifieds. On March 31, 2017, Nex-Tech COO Michael Pollock reported to Ridgway that their service had been a victim of a Distributed Denial of Services (DDOS) attack. A DDOS occurs when "multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple comprised systems (for example, a botnet) flooding the targeted system with traffic." (Doc. 25, Exh. A at 2.) This results in preventing Nex-Tech customers from accessing the website. Ridgway conducted an investigation and reviewed Nex-Tech's records.

Notably, prior to the attacks, Nex-Tech received threats. On March 27, 2017, a user identified as "grass_is_green" sent two threats by a Nex-Tech e-form contact within just a few minutes. The first threat stated:

> take my ad down again when my description dosnt violate copy right, i will violate this site by bringing it offline, fix the ad. if u make me upset, i will retaliate, your choice, and im not making a threat im capable of bringing down this website

(*Id.*, ¶ 14 l.) (spelling, capitalization, and grammar errors in original).

The second threat stated: "ip address 24.225.8.90 will be submitted at exostress. in for 24 hours if my demands are not met with in (sic) 12 hours, your choice, and remember you have been

warned." (Id., ¶ 14 m.) The "grass_is_green" account was created on March 25 with an email address of ntcsucks@mail.com and a contact number of xxx-xxx-1011.[2] On March 25, "grass_is_green" posted an ad for a 1200cc Suzuki Bandit motorcycle. The IP address that was used by "grass_is_green" was 69.98.202.80, which was the static IP address for the Pawnee County Courthouse ("Courthouse IP"). Shortly after the first posting, "grass_is_green" posted an ad for a "jailbrokenPS3," using the same IP address and the same contact number. This ad was rejected by Nex-Tech for violating Nex-Tech's terms of service.

On March 26, the user "water_is_blue" was created with an e-mail address of janentcsucks@mail.com. The city listed for the user is Larned, Kansas. Within the same hour of creating the user name, the user contacted another classified user and accessed the internet through Courthouse IP. That same evening, "grass_is_green" contacted other classified users from an electronic device accessing the internet by using the IP address 68.99.114.67. This IP address was the static IP address assigned to the Jordaan Memorial Library ("Library IP.")

On March 27, after sending the threats, "grass_is_green" sent another user a message by utilizing the Library IP to access the internet. Nex-Tech deactivated the "grass_is_green" account shortly after this message was sent. Later that morning, "water_is_blue" posted an advertisement for a 1200cc Suzuki Bandit motorcycle using the Library IP. On March 29, "water_is_blue" posted an advertisement for a PlayStation 3 using a different IP address. The contact phone number listed was xxx-xxx-1011. Shortly thereafter, the posting was rejected for violating the terms of service.

On March 30, "water_is_blue" posted an advertisement for a PlayStation 3 from the Library IP address. The contact phone number listed was xxx-xxx-1011. Again, the posting was

[2] An account was created with the user name "banditnut598" on February 25, 2017. This user was later deactivated by Nex-Tech for violations of the terms of service due to using profanity and abusive behavior. This user also provided the phone number xxx-xxx-1011 and accessed the internet through the same IP addresses as "grass_is_green."

rejected for violating the terms of service. "Water_is_blue" then contacted the help desk to inquire as to the reason for the rejection. Later that evening, from 8:50 to 9:10 p.m., a DDOS attack occurred which prevented customers from accessing the Nex-Tech classifieds web site. Between 9:02 and 9:07 p.m., the user "water_is_blue" called the Nex-Tech Help Desk and asked for an explanation as to why the advertisement was rejected. The call was disconnected when the technician tried to look up the notes and the website was down. Another DDOS attack occurred between 9:18 and 9:37 p.m. that prevented customers from accessing the website. "Water_is_blue" called the help desk again during this time. During the call, the user asked where the Nex-Tech websites were located, where the company was located, and left a call back number of xxx-xxx-1011.

On March 31, a third attack occurred that prevented customers from accessing the website for one hour and resulted in a loss of revenue to Nex-Tech. Two more attacks occurred that day against the Nex-Tech classifieds site. Two attacks also occurred against Nex-Tech's corporate website which resulted in Nex-Tech being unable to "monitor circuits and network equipment for many public safety entities (hospitals, law enforcement, fire stations, etc.) and medical alert customers." (Doc. 25, Exh. A at ¶ 14bb.) On April 6, the Nex-Tech Classifieds' server was accessed by an electronic device accessing the internet from the Library IP.

Upon a search of Nex-Tech's records, it was discovered that user "larned_seller" listed the contact number of xxx-xxx-1011, during a November 2014 communication with another user. The account "larned_seller" was created in November 2014. The user "larned_seller" also provided the address of 714 1/2 Topeka Street in Larned, Kansas, in order to facilitate an exchange of items purchased from "larned_seller."

Ridgway determined that the 714 ½ Topeka address was owned by John Golightley. John Golightley's driver's license listed a home address on Mark Avenue in Larned. Defendant's driver's license, dated March 3, 2017, listed an address of 714 1/2 Topeka. The distance between the Library and the Topeka residence is approximately 100 yards. The distance between the Courthouse and the Topeka residence is approximately 200 yards.

Additionally, on June 29, 2011, Robert Blackwell, previously an officer with the Edwards County Sheriff's Office, completed a written statement concerning Defendant. In that statement, Blackwell stated that Defendant informed him that he had built a device, "best described as a make-shift satellite dish, capable of broadcasting a wireless signal out an incredibly long range. [Defendant] explained he used this device to access the" County's Courthouse wireless network. (*Id.* at ¶ 27b.)

Judge Braun authorized the search warrant. The items to be seized included the following:

> 1. Computers, laptops, cellular phones, tablets, or other mobile devices capable of being used to access the internet based Nex-Tech Classified system;
> 2. Hard disk drives, compact disks (CDs), digital video disks (DVDs), flash memory drives, or any other digital storage medium capable of storing data relating to the to [sic] access of the internet based Nex-Tech Classified system;
> 3. Papers, documents, receipts, or other written instruments tending to demonstrate purchases, sales, or ownership equipment used to access of [sic] the internet based Nex-Tech Classified system.
> 4. Antennas, dishes, range extenders, range boosters and other equipment used for the purpose improving [sic] and extending the usable distance of wireless communication devices.
> 5. Correspondence or other documents (whether digital or written) pertaining to the use of the internet based Nex-Tech Classified system;
> 6. Items or digital information that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts and cellular digital networks to access the internet based NexTech Classified system.

(Doc. 25, Exh. A at 1.)

At the hearing, Ridgway testified that a meeting was held with the officers who would be participating in the execution of the search warrant. The items to be seized were discussed and it

was made clear that only these items were to be seized. The officers then executed the search warrant for 714 1/2 Topeka. The return indicates that the items seized include a laptop, cellular phone, flash drives, modem, and other items. (Doc. 30, Exh. 1-A.)

During the execution of the search warrant for 714 1/2 Topeka, officers also discovered a "battery type device" located in the front room of Defendant's residence. (Doc. 25, Exh. B. at ¶ 28.) There was a cable attached to the device which exited Defendant's residence and eventually went underground. It then resurfaced at the southwest corner of a metal shed located on 714 Topeka Street, Larned, Kansas, and entered the shed. There was a solar panel on the shed's roof. An officer was informed by the property's owner, John Golightley, that the shed was used by Defendant and that the owner did not have access to the shed.

Ridgway included the new information on a search warrant for the shed at 714 Topeka Street. Judge Braun authorized the search of the shed. The officers executed the warrant on the same day, May 24, but did not seize any property. (Doc. 30, Exh. 2-A.)

Defendant moves to suppress the evidence seized pursuant to the warrant on the basis that it lacked probable cause, a sufficient nexus to the crime, and particularity.

II. Analysis

A. Probable Cause

The Fourth Amendment to the United States Constitution provides that:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The validity of a warrant is not determined by "nit-picking" discrete portions of the application. Rather, the test is whether, under the totality of the circumstances presented in the affidavit, the issuing judge had a "substantial basis" for determining that probable

cause existed. *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983); *United States v. Harris*, 369 F.3d 1157, 1165 (10th Cir. 2004) ("In determining whether a search warrant was supported by probable cause, we review 'the sufficiency of the affidavit upon which a warrant [wa]s issued by looking at the totality of the circumstances and simply ensuring 'that the [issuing] magistrate had a substantial basis for concluding that probable cause existed.'" (internal citation omitted)). The court gives great deference to a search warrant that was reviewed and signed by an experienced judge. *See United States v. Leon*, 468 U.S. 897, 914 (1984); *United States v. Price*, 265 F.3d 1097, 1101 (10th Cir. 2001).

Probable cause exists when "the facts presented in the affidavit would warrant a man of reasonable caution to believe that evidence of a crime will be found at the place to be searched." *Harris*, 369 F.3d at 1165 (quoting *United States v. Hernandez-Rodriguez*, 352 F.3d 1325, 1330 (10th Cir. 2003)). The Tenth Circuit has adopted the general rule that probable cause requires a "nexus between [the contraband to be seized] or suspected criminal activity and the place to be searched." *United States v. Rowland*, 145 F.3d 1194, 1203 (10th Cir. 1998) (quoting *United States v. Corral-Corral*, 899 F.2d 927, 937 (10th Cir. 1990)).

Defendant argues that the affidavit does not provide facts that a DDOS attack occurred nor does it state facts that would allow a reasonable person to conclude that the crime was carried out by Defendant or in his home on Topeka. (Doc. 25 at 6.)

Violation of K.S.A. 21-5839. With respect to the crime at issue, the affidavit states that the crime allegedly committed was a violation of K.S.A. 21-5839. That statute provides as follows:

> (a) It is unlawful for any person to:
> (1) Knowingly and without authorization access and damage, modify, alter, destroy, copy, disclose or take possession of a computer, computer system, computer network or any other property;
> (2) use a computer, computer system, computer network or any other property for the purpose of devising or executing a scheme or artifice with the intent to defraud or to obtain

> money, property, services or any other thing of value by means of false or fraudulent pretense or representation;
> (3) knowingly exceed the limits of authorization and damage, modify, alter, destroy, copy, disclose or take possession of a computer, computer system, computer network or any other property;
> (4) knowingly and without authorization, disclose a number, code, password or other means of access to a computer, computer network, social networking website or personal electronic content; or
> (5) knowingly and without authorization, access or attempt to access any computer, computer system, social networking website, computer network or computer software, program, documentation, data or property contained in any computer, computer system or computer network.

K.S.A. 21-5839.

Defendant is correct that the probable cause finding cannot be based on wholly conclusory statements. *See Gates*, 462 U.S. at 239. This court must disregard any conclusory statements in reviewing a warrant for probable cause. *Id.* Although the affidavit makes several references to DDOS attacks, the affidavit does not solely rely on the assertion that an attack occurred. Rather, there are several factual statements that support a finding that those attacks did occur.

The affidavit states that there were two threats to Nex-Tech that stated the "grass_is_green" user was going to bring the website down if certain ads were not restored. Only three days after those threats were issued, Nex-Tech Classifieds' site experienced a DDOS attack. The affidavit states that website traffic prevented customers from accessing the website. The affidavit sets forth facts concerning additional attacks to the Nex-Tech corporate website which resulted in an inability to monitor circuits and network equipment for many public safety entities. The affidavit clearly defined an attack as flooding the bandwidth on a website that is done by a botnet, which is a network of private computers infected with malicious software and controlled without the owners' knowledge. (Doc. 25, Exh. A at 2.)

These facts were sufficient to provide the state court judge with probable cause to believe that a violation of K.S.A. 21-5839 had occurred.

Sufficient Nexus. Defendant further argues that the affidavit fails to sufficiently connect the alleged criminal activity to 714 1/2 Topeka. In addition to facts sufficient to support probable cause that a crime occurred, there must be a nexus between the suspected criminal activity and the place to be searched. *Rowland*, 145 F.3d at 1203. The affidavit is not required to "draw an explicit connection between a suspect's activities and his residence for a Fourth Amendment nexus to exist." *United States v. Biglow*, 562 F.3d 1272, 1280 (10th Cir. 2009). A state court judge may draw reasonable conclusions based on the affidavit and "practical considerations of everyday life." *Id.*

Defendant argues that the connection between the different registered users is weak and that the information regarding the address used in 2014 and the police report in 2011 is stale. Based on the facts set forth in the affidavit, there is strong evidence of a connection between the users "banditnut598", "grass_is_green", and "water_is_blue." This is evidenced by Defendant's chart contained at page 10 of his brief. (Doc. 25 at 10.) The accounts all accessed the internet using the Library IP and the Courthouse IP. They all had the same phone number and all placed similar ads for the same items. Therefore, it is reasonable for the state court judge to infer that these users were the same individual. Defendant, however, argues that the larned_seller account connection is weak and the information stale. One common fact connecting the larned_seller account with the other three user accounts is the phone number. But this is not the only connection tying the user accounts together. As set forth in the affidavit, larned_seller is associated with the address 714 1/2 Topeka. All three other user accounts accessed the internet from the Library and the Courthouse. This is significant as those locations are only 100 and 200 yards, respectively, from 714 1/2 Topeka. Therefore, in addition to sharing the same phone number, user larned_seller's address is within only 200 yards, at most, of the location of the wireless access

points through which the three other users were accessing the internet. This fact makes it reasonable to infer that all four users are the same individual.

Based on that inference, it was reasonable to infer that evidence of the crime would be found at the Topeka Street address. This address was given by larned_seller in order to sell an item to another user. The address is also only 100 yards from the Library and 200 yards from the Courthouse, which are the locations where the internet network was accessed. Additionally, Defendant has stated in the past that he accessed the internet from the Courthouse using a device that he built. Although this information was from 2011, Defendant's driver's license, which was dated in 2017, identified his home address as the Topeka address. It is reasonable to infer, based on recent activities of the three user names at Nex-Tech, that Defendant continues to use some type of device to access the internet from the Library and the Courthouse's networks. Moreover, although Defendant argues that laptops and cell phones are transient, it was entirely reasonable for the state court judge to infer that the computers, phones, or other internet capable devices used in the alleged offense would be located in the Topeka residence.

In *Biglow*, the Tenth Circuit identified a non-exhaustive list of factors relevant to the nexus determination, including: "(1) the type of crime at issue, (2) the extent of a suspect's opportunity for concealment, (3) the nature of the evidence sought, and (4) all reasonable inferences as to where a criminal would likely keep such evidence." *Id.* at 1279. As discussed, this is a crime that is committed by a device that is capable of accessing the internet. The evidence sought is a computer or related device and all reasonable inferences would suggest that computers or related devices are often kept in the home. Therefore, considering the facts in the affidavit and all reasonable inferences that can be made from those facts, the court finds that there is a sufficient nexus between the suspected criminal activity and the place to be searched.

In the event that the affidavit lacked probable cause, the court concludes that "the affidavit's information nonetheless provided sufficient indicia of probable cause to justify the officers [sic] good-faith reliance." *Campbell*, 603 F.3d at 1233. It is presumed that an officer acts in good-faith reliance when executing a search warrant. *United States v. Augustine*, 742 F.3d 1258, 1262 (10th Cir. 2014). "This presumption, though not absolute, 'must carry some weight.'" *United States v. Harrison*, 566 F.3d 1254, 1256 (10th Cir. 2009). When an affidavit "describes circumstances which would warrant a person of reasonable caution in the belief that the articles sought are at a particular place," the Tenth Circuit has found "objectively reasonable reliance on an affidavit's establishment of a nexus." *United States v. Ejiofor*, 753 F. App'x 611, 616–17 (10th Cir. 2018) (citing *Augustine*, 742 F.3d at 1263). Because the affidavit included facts that connected the 714 1/2 Topeka house to the user accounts, and because it is reasonable to believe that computers and other internet accessible devices could be found in Defendant's home, the court finds that the officers acted in good-faith reliance on the sufficiency of the warrant.

B. Particularity

Finally, Defendant argues that the warrant is not sufficiently particular because it sought a "massive swath of digital content from Michael's home." (Doc. 25 at 14.)

The Fourth Amendment requires not only that warrants be supported by probable cause, but that they "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

> A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized. Even a warrant that describes the items to

> be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit. However, the Fourth Amendment requires that the government describe the items to be seized with as much specificity as the government's knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized.

United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988) (internal citations omitted).

Defendant cites *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999), in support of the position that this warrant is deficient in not placing a "meaningful limit" on the type of media seized. (Doc. 25 at 15.) *Carey*, however, was addressing a search warrant which allowed the officers "to search the files on the computers for 'names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.'" *Carey*, 172 F.3d at 1270 ("Mr. Carey complains: (1) search of the computers exceeded the scope of the warrant, (2) he did not consent to the search of his apartment, and (3) seizure of the computers was unlawful because the officers lacked probable cause. We address only the first issue.") The warrant at issue here did not pertain to the actual searching of the electronic devices. Defendant has not cited to any authority that suggests that the language used in this warrant, which specifies devices that can access the internet or devices that are capable of storing data relating to the access of the internet, is too broad. Nor has Defendant identified language that would be sufficient here. Both Ridgway and Detective Shirley-Williams testified that there is no way to further limit the language because they are unable to determine what type of device was used in this instance to commit the crime at issue. The court finds that the "description is as specific as the circumstances and the nature of the activity under investigation permit." *Leary*, 846 F.2d at 600. Therefore, this warrant complies with the Fourth Amendment.

Speaker. At the hearing, Defendant raised an additional argument regarding the seizure of a speaker. Ridgway testified that he seized the speaker and, at the time, did not know what it was.

Ridgway admitted that the speaker does not fall within the items to be seized. "As a general rule, only the improperly seized evidence, not all of the evidence, must be suppressed, unless there was a flagrant disregard for the terms of the warrant." *United States v. One Hundred Forty-Nine Thousand Four Hundred Forty-Two & 43/100 Dollars ($149,442.43) in U.S. Currency*, 965 F.2d 868, 875 (10th Cir. 1992). Here, there is no evidence that there was a flagrant disregard for the terms of the warrant. With the exception of the speaker, all items seized fell within the warrant. The seizure of the speaker did not turn the search into a general search. *Id.* Therefore, the speaker is inadmissible at trial.[3]

III. Conclusion

Defendant's motion to suppress (Doc. 25) is DENIED IN PART AND GRANTED IN PART. The speaker, Ear Force DSS2 Dolby Surround Sound Processor, is suppressed. Defendant's motion to suppress all other evidence seized during the execution of the warrant at 714 1/2 Topeka is denied.

IT IS SO ORDERED.

Dated this 2nd day of April, 2019.

s/ John W. Broomes
JOHN W. BROOMES
UNITED STATES DISTRICT JUDGE

[3] At a subsequent hearing, the government informed the court that it does not intend to offer the speaker into evidence at trial.